

© Н.К. Круглов, А.С. Зуфарова

Научная статья
УДК 37.01:007

ПРОТИВОДЕЙСТВИЕ ФИШИНГУ: ОБУЧЕНИЕ И ЗАЩИТА С ПОМОЩЬЮ ПЛАТФОРМЫ PHISHINGTRAINER И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Н.К. Круглов, А.С. Зуфарова

Круглов Никита Константинович,
студент, Тихоокеанский государственный
университет, Хабаровск, Россия.
2020104710@togudv.ru

Зуфарова Анна Сергеевна,
старший преподаватель кафедры математических
методов защиты информации и компьютерной
безопасности, Тихоокеанский государственный
университет, Хабаровск, Россия.
006694@togudv.ru

Аннотация. В условиях стремительной цифровизации бизнеса фишинг остаётся одной из самых распространённых и опасных киберугроз. Злоумышленники всё чаще используют социальную инженерию, поддельные сайты и технологии искусственного интеллекта для создания убедительных атак, нацеленных на сотрудников компаний. При этом даже самые современные технические средства защиты не дают стопроцентной гарантии безопасности, если персонал не обучен распознавать признаки мошенничества. Именно поэтому противодействие фишингу требует комплексного подхода, сочетающего технологические инструменты и системное обучение. В связи с этим возникает необходимость в эффективной подготовке сотрудников к противодействию таким угрозам. Платформа «PhishingTrainer» представляет собой инновационное решение в области кибербезопасности, интегрирующее передовые методы машинного обучения для обучения сотрудников основам информационной безопасности. Система разрабатывает индивидуализированные учебные материалы, основанные на фишинговых ссылках, что позволяет адаптировать процесс обучения к уникальным потребностям и уровню подготовки каждого сотрудника. Это достигается за счёт использования алгоритмов искусственного интеллекта, способных анализировать поведенческие паттерны и предпочтения пользователей, обеспечивая тем самым максимальную эффективность и персонализацию обучения. Платформа PhishingTrainer позволяет организациям не только моделировать реальные сценарии атак, но и формировать устойчивые навыки кибербезопасного поведения у сотрудников с использованием возможностей искусственного интеллекта. Такой подход помогает минимизировать риски и повысить общий уровень информационной безопасности компании. В данной статье приведен опрос о знаниях о фишинге. Рассмотрены основы создания обучающей платформы, принципы работы и учебные материалы. Результаты исследования демонстрируют, что комплексный подход, сочетающий технологические средства защиты и регулярное интерактивное обучение, значительно снижает вероятность успешных фишинговых атак, повышает уровень

информационной безопасности организации и формирует культуру осознанного отношения к цифровым рискам.

Ключевые слова: *кибербезопасность, фишинговые атаки, обучение, искусственный интеллект, обучающая платформа, образовательные технологии.*

Библиографическая ссылка: *Круглов Н.К., Zufarova A.S. Противодействие фишингу: обучение и защита с помощью платформы PhishingTrainer и искусственного интеллекта // ЦИТИСЭ. 2026. № 1. С. 634-647.*

Research Full Article

UDC 37.01:007

COUNTERING PHISHING: TRAINING AND PROTECTION USING THE PHISHINGTRAINER PLATFORM AND ARTIFICIAL INTELLIGENCE

N.K. Kruglov, A.S. Zufarova

Nikita K. Kruglov,

student, Pacific State University, Khabarovsk,
Russian Federation.
2020104710@togudv.ru

Anna S. Zufarova,

Senior Lecturer at the Department Mathematical
Methods of Information Security and Computer
Security, Pacific State University, Khabarovsk,
Russian Federation.
006694@togudv.ru

Abstract. *In the context of rapid digitalization of business, phishing remains one of the most widespread and dangerous cyber threats. Attackers are increasingly using social engineering, fake websites, and artificial intelligence technologies to create convincing attacks targeting company employees. At the same time, even the most modern technical means of protection do not provide an absolute guarantee of security if the personnel is not trained to recognize signs of fraud. That is why countering phishing requires an integrated approach combining technological tools and systematic training. In this regard, there is a need for effective training of employees to counter such threats. The PhishingTrainer platform is an innovative cybersecurity solution that integrates advanced machine learning techniques to teach employees the basics of information security. The system develops customized training materials based on phishing links, which allows you to adapt the learning process to the unique needs and level of training of each employee. This is achieved through the use of artificial intelligence algorithms capable of analyzing user behavioral patterns and preferences, thereby ensuring maximum effectiveness and personalization of training. The PhishingTrainer platform allows organizations not only to simulate real-world attack scenarios, but also to develop sustainable cybersecurity skills among employees using artificial intelligence capabilities. This approach helps to minimize risks and increase the overall level of information security of the company. This article contains a survey on knowledge about phishing. The basics of*

creating a training platform, principles of operation and training materials are considered. The results of the study demonstrate that an integrated approach combining technological protection tools and regular interactive training significantly reduces the likelihood of successful phishing attacks, increases the level of information security of an organization and creates a culture of conscious attitude to digital risks.

Keywords: *cybersecurity, phishing attacks, training, artificial intelligence, learning platform, educational technologies.*

For citation: Kruglov, N. K., & Zufarova, A. S. (2026). Countering phishing: Training and protection using the PhishingTrainer platform and artificial intelligence. *CITISE, 1*, 634–647. (In Russian).

Введение.

Человеческий фактор был и остается самым слабым звеном в системе информационной безопасности. Несмотря на все более сложные системы защиты, злоумышленники успешно обходят их, используя методы социальной инженерии, среди которых фишинг является самым массовым. Стандартные подходы к обучению пользователей, такие как инструктажи и однотипные учебные фишинговые рассылки, зачастую не способны сформировать устойчивые навыки распознавания реальных угроз, которые постоянно эволюционируют [1].

Парадокс современной кибербезопасности заключается в том, что для эффективного обучения защите от фишинга необходимо моделировать атаки, максимально приближенные к реальным. Однако создание таких реалистичных сценариев для каждого сотрудника вручную требует неоправданно высоких временных и трудовых затрат. На помощь приходят технологии искусственного интеллекта, а именно машинное обучение, которое позволяет автоматизировать процесс создания целевого и персонализированного контента.

Актуальность данной темы обусловлена стремительным ростом киберугроз в современном цифровом мире и критической важностью человеческого фактора в системе информационной безопасности. Фишинг остается одним из самых распространенных и деструктивных методов атак, а традиционные подходы к обучению пользователей демонстрируют свою недостаточную эффективность. Использование машинного обучения для генерации персонализированных учебных материалов позволяет решить данную проблему. Этот подход позволяет учитывать уникальные особенности каждого испытуемого, такие как уровень знаний, стиль обучения и интересы, что значительно повышает эффективность образовательного процесса.

Платформа «PhishingTrainer» — это программный тренажер, который использует машинное обучение для генерации персонализированных атак, которые повышают уровень осведомленности сотрудников и минимизируют риски подверженности фишинговым атакам.

В настоящее время термин «фишинг» не определен ни в одном нормативно-правовом акте РФ. Под фишингом понимается вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей [2]. Злоумышленники рассчитывают, что пользователи, попадая на поддельные сайты, не заметят подделки и добровольно введут свои личные данные. В настоящее время в Российской Федерации формируется единая платформа, обеспечивающая взаимодействие всех заинтересованных сторон в целях противодействия мошенничеству с использованием фишинговых атак и повышению приватности для граждан, бизнеса и должностных лиц [3]. Согласно техническому заданию от Минцифры, под фишинговым сайтом понимается «информационный ресурс в сети Интернет, схожий до степени смешения с сайтами известных брендов, часто сайтами банков и других финансовых институтов, специально созданный злоумышленниками с целью

введения в заблуждение пользователей для завладения их личными данными и совершения в отношении них мошенничества» [4].

Для подтверждения актуальности темы был проведен опрос на тему «Fishing», который проверял уровень осведомленности противодействию фишинговым атакам среди пользователей сети Интернет. Общее количество опрошенных составляет 149 человека, среди них большая часть студентов и школьников (133 человека), IT-сотрудник (1 человек), сотрудников, чья деятельность не связана с IT (9 человек), а также пенсионер (1 человек), диаграмма градации по возрасту представлена на рисунке 1.

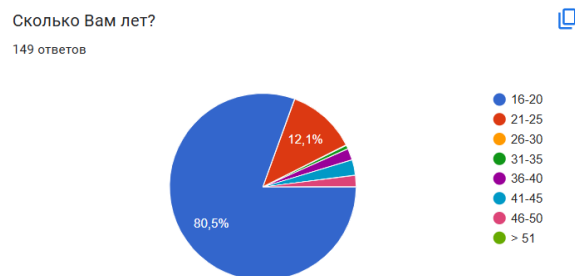


Рисунок 1 — Диаграмма опроса

Анализ результатов тестирования осведомленности о фишинговых атаках, представленный на рисунке 2, выявил ряд тревожных тенденций, подтверждающих актуальность данного исследования. Несмотря на относительно высокий средний балл (7-10), ключевой проблемой является значительная поляризация знаний среди пользователей. Наличие устойчивой группы лиц, показавших крайне низкие результаты (0–3 балла), свидетельствует о наличии «человеческого фактора» как критического вектора кибератак. Широкий разброс результатов (от 1 до 10 баллов) указывает на неэффективность унифицированных подходов к обучению. Таким образом, актуальность настоящей работы заключается в разработке целенаправленных мер по выявлению и повышению уровня киберграмотности среди наиболее уязвимых пользователей, что в конечном итоге позволит снизить общие риски успешных фишинговых атак.

Статистика

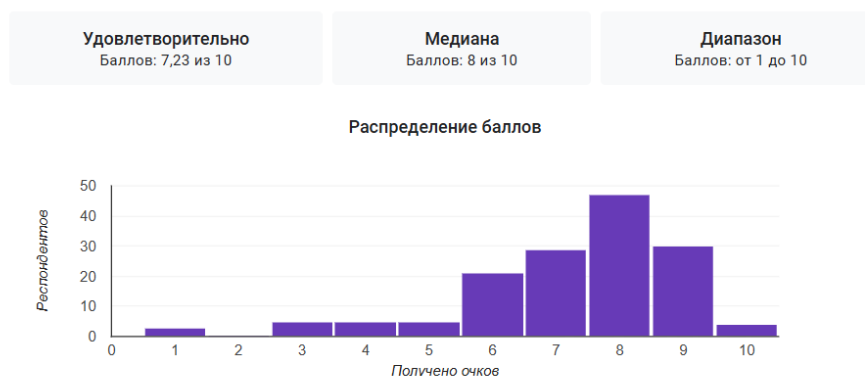


Рисунок 2 - Статистика пройденного опроса

На рисунке 3 представлены два вопроса, на которые меньше всего дано правильных ответов. Исходя из данного результата, можно сказать, что большинство респондентов не

полностью осведомлены о каналах фишинга и как правильнее всего действовать в случае взлома знакомых.

❗ Вопросы, на которые часто даются неправильные ответы ?

Вопрос	Правильные ответы
Какие каналы чаще всего используются для фишинга?	28/149
В мессенджеры вам пишет друг и просит срочно одолжить денег на карту, так как его телефон "сломался и он сидит с чужого". Он просит не звонить	41/149

Рисунок 3 — Вопросы, на которые чаще остальных давали неверные ответы

Был задан вопрос «Какие каналы чаще всего используются для фишинга?» 27,5 % ответили, что только электронная почта, 77,9 % мессенджеры, 83,2%, что социальные сети и 47,7% через телефон. Каналы для фишинга могут быть любыми и сотрудники и обучающиеся, должны знать об этом и уметь определить фишинг. Данные опроса представлен на рисунке 4.

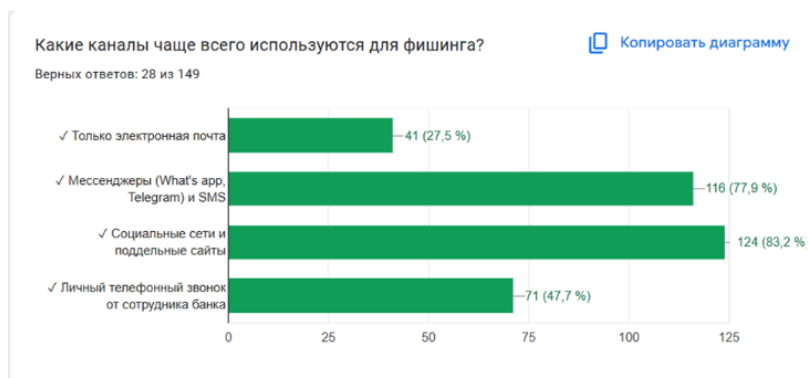


Рисунок 4 — Результат опроса «Какие каналы чаще всего используются для фишинга?»

Следующий заданный вопрос был, про мессенджеры. Результат представлен на рисунке 5.

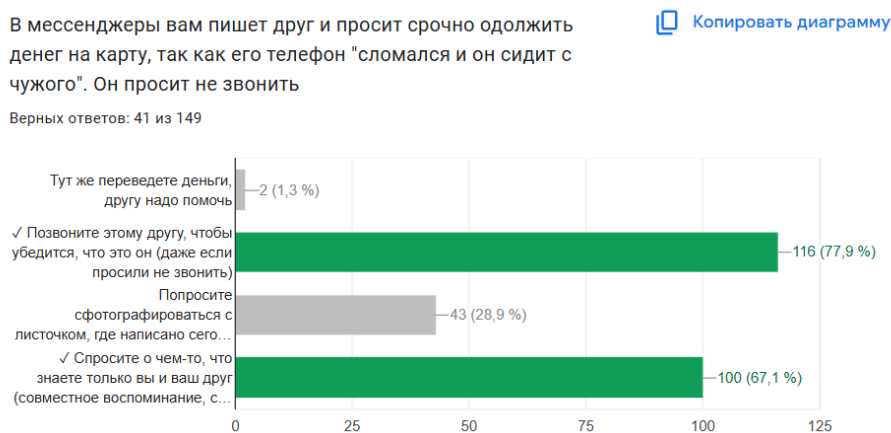


Рисунок 5 — Результат опроса

Результаты опроса доказывают, что тема фишинга актуальна и по сей день.

Основная часть.

В условиях цифровизации профессиональной деятельности сотрудники организаций ежедневно взаимодействуют с электронной почтой, корпоративными порталами и облачными сервисами. Это делает их основной мишенью фишинговых атак — одной из самых распространённых форм социальной инженерии. Однако практика показывает, что технические средства защиты не обеспечивают полной безопасности без сформированной киберграмотности персонала. Следовательно, ключевая задача состоит не только в внедрении защитных технологий, но и в построении системной образовательной среды, направленной на формирование устойчивых поведенческих навыков безопасного взаимодействия с цифровой информацией. Одним из эффективных решений является создание обучающей платформы, использующей имитационные фишинговые ссылки как педагогический инструмент [5].

Обучение взрослых сотрудников относится к сфере андрагогики. Взрослые обучающиеся: лучше усваивают материал, связанный с их профессиональной деятельностью; эффективнее обучаются через практический опыт; нуждаются в понимании практической значимости изучаемого материала; воспринимают обучение как инструмент решения реальных задач [6].

Поэтому традиционные лекционные форматы в области информационной безопасности демонстрируют низкую эффективность. Гораздо более результативным является обучение через моделирование ситуаций, максимально приближённых к реальным [7; 8].

Создание платформы для обучения сотрудников по защите от фишинга с использованием фишинговых ссылок имеет важное значение в современном цифровом мире. Тренажер-платформа «PhishingTrainer» предоставляет уникальные возможности для имитации реальных угроз и повышения уровня осведомленности сотрудников. Платформа оснащена искусственным интеллектом и ориентируется на должность сотрудников для более индивидуального подхода к каждому сотруднику. Один из блоков — это наличие машинного обучения для генерации учебных фишинговых писем для сотрудников, ориентируясь на их интересы и увлечения. Ниже на рисунке 6 представлена блок-схема платформы «PhishingTrainer» с описанием ключевых компонентов и потоков данных.

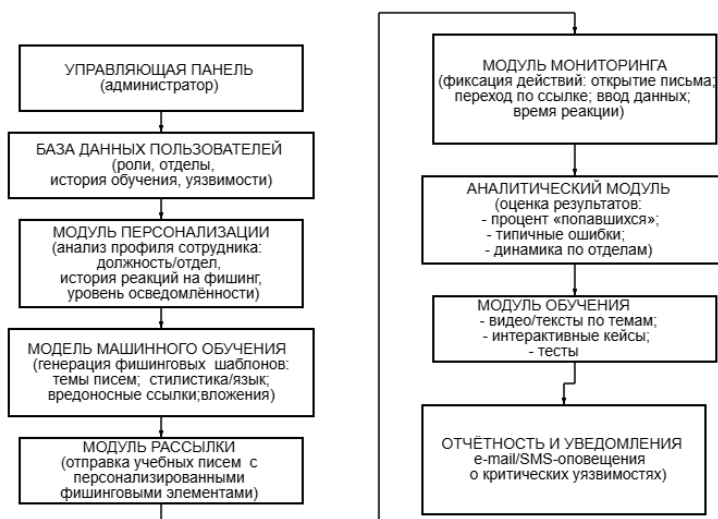


Рисунок 6 — Блок-схема платформы «PhishingTrainer»

Данный выбранный программно-технологический стек обеспечил разработку адаптивной платформы обучения с элементами искусственного интеллекта, способной генерировать персонализированные сценарии фишинговых атак при сохранении простоты развертывания и оптимальных вычислительных требований.

Структура обучающей платформ, с педагогической точки зрения, она должна включать следующие компоненты: диагностическую модель, модуль ситуационного обучения, рефлексивный модуль, модуль закрепления знаний.

Диагностический модуль, позволяет определить исходный уровень осведомлённости сотрудников через тестирование и симуляционные кампании. Ситуационный модуль обучения включает в себя: рассылка имитационных писем; фиксация действий сотрудников; автоматическое перенаправление на обучающий материал. Рефлексивный модуль включает в себя: анализ совершённых ошибок; объяснение признаков фишинга; рекомендации по корректному поведению. Модуль закрепления знаний: интерактивные тесты; кейс-задания; повторные симуляции.

На рисунке 7 представлена стартовая страница, куда попадает сотрудник, который ищет универсальное решение для повышения осведомленности своих сотрудников в области противодействия фишинговым атакам.

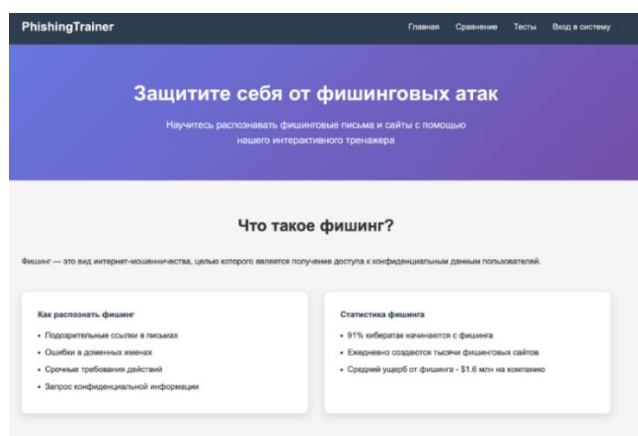


Рисунок 7 — Стартовая страница платформы

На рисунке 8 представлена страница администратора системы, в которой он может добавлять новых пользователей и испытуемых. Здесь указываются данные для дальнейшей авторизации пользователя, а также организация, в которой работает пользователь, для дальнейшей персонализации фишинговых писем сотрудникам.

Рисунок 8 — Страница регистрации новых пользователей

На рисунке 9 представлена система управления созданными пользователями и испытуемыми, где все участники системы распределены по организациям для удобства

администрирования пользователями. На данной странице администратор системы может удалять сотрудников и испытуемых из системы.

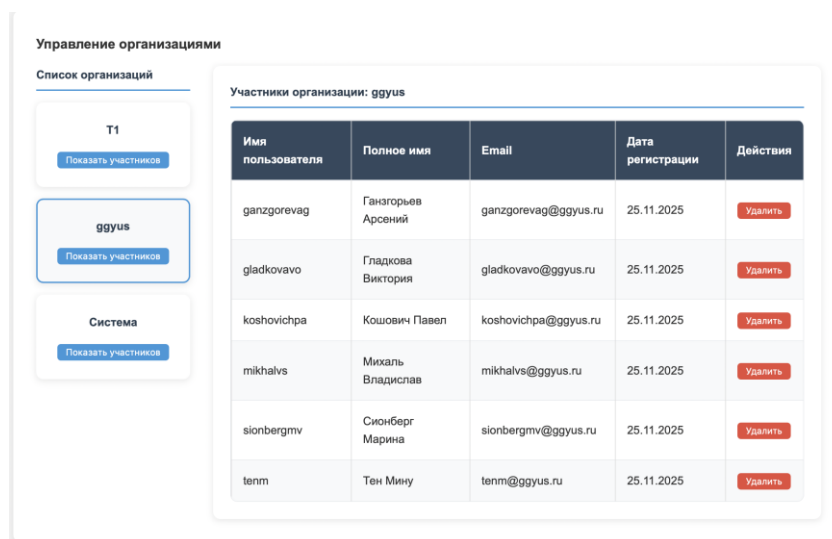


Рисунок 9 — Система управления созданными пользователями

На рисунке 10 представлена страница администрирования для пользователей организаций, где они могут добавлять испытуемых. Здесь также разграничена установка организации, для того чтобы пользователь не мог добавлять сотрудников из другой организации.

Добавить участника информационного обмена

Имя пользователя: Email:

Полное имя: Пароль:

Организация:

Организация назначается автоматически

[Добавить участника](#)

Участники вашей организации

Имя пользователя	Полное имя	Email	Роль	Дата регистрации	Действия
user123	123	123@mail.ru	ИСПЫТУЕМЫЙ	12.10.2025	Удалить

Рисунок 10 - Страница администрирования испытуемыми

На рисунке 11 представлена страница личного кабинета испытуемого, где он может наблюдать свой прогресс обучения, количество пройденных тестов, а также успешность пройденных испытаний.

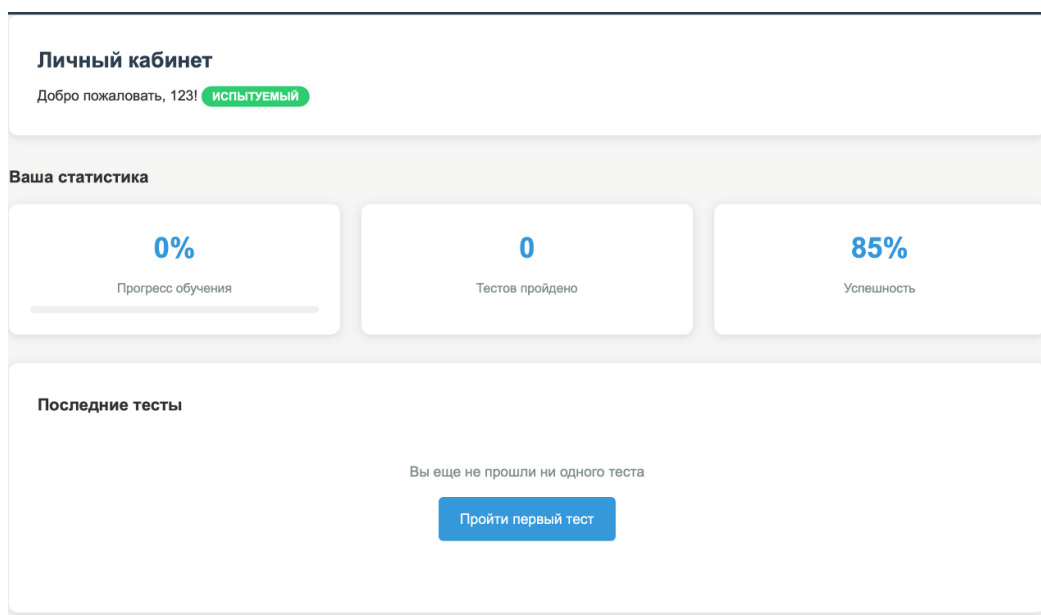


Рисунок 11 — Личный кабинет испытуемого

В момент создания аккаунта испытуемого пользователю необходимо указать возможные интересы сотрудника, личную электронную почту, мессенджеры, которыми пользуется испытуемый. Данная информация обрабатывается на сервере, где проходит анализ возможных интересов сотрудника. Программа анализирует, на каких ресурсах зарегистрирован испытуемый, какую занимает должность, а также возраст испытуемого для генерации персонализированного письма. После анализа входных данных программа начинает, используя машинное обучение, генерировать письмо для сотрудника. В данном письме программа, ориентируясь на интересы пользователя, подгоняет персонализированное письмо и вставляет туда «фишинговую» ссылку, перейдя на которую пользователь не потеряет свои данные, но увидит, что его только что пытались взломать. После отправки всех писем руководитель видит график, кто перешел по «фишинговой» ссылке, и может назначать для этих сотрудников обучающие модули.

Для генерации писем была использована предобученная модель `rugpt3small_based_on_gpt2`, разработанная Sberbank AI.

Модель `rugpt3small_based_on_gpt2` основана на архитектуре трансформера, которая была впервые представлена в статье "Attention is All You Need" (2017) и впоследствии использована в модели GPT-2. В этой архитектуре ключевую роль играет механизм внимания (*attention mechanism*), который позволяет модели эффективно обрабатывать последовательности текста и учитывать контекст [9]. Модель может быть использована для генерации писем, например, для автоматизации отправки уведомлений, приглашений или других типов сообщений. Она также может быть интегрирована в системы поддержки клиентов для генерации ответов на запросы пользователей.

Данный выбор обусловлен несколькими ключевыми факторами. Во-первых, модель специально обучена на русскоязычных текстах, что обеспечивает корректную генерацию с учетом особенностей русской грамматики, синтаксиса и стилистики.

Во-вторых, архитектура GPT-2 хорошо зарекомендовала себя в задачах генерации связного текста, сохраняя контекст и логическую последовательность предложений. Важным преимуществом стало то, что модель предлагает оптимальный баланс между качеством генерации и вычислительной эффективностью: будучи достаточно компактной для быстрого интерфейса, она сохраняет способность создавать осмысленные и разнообразные тексты. Кроме того, использование готовой предобученной модели исключает необходимость

трудоемкого процесса дообучения на собственных данных, что значительно ускоряет развертывание системы. Интеграция технологий искусственного интеллекта позволяет усилить педагогический эффект: автоматическая генерация реалистичных сценариев; адаптация сложности заданий; выявление поведенческих закономерностей; формирование индивидуальных образовательных траекторий. ИИ обеспечивает переход от стандартного обучения к адаптивной модели, где содержание подстраивается под конкретного сотрудника.

Пример сгенерированного письма для сотрудника Ганзгорьев Арсений возраст: 60 лет, город: Южно-Сахалинск, интересы: рыбалка, спорт, охота (рисунок 12).

Уважаемый Арсений!

Компания «Охотник» с большим уважением обращается к вам, зная о вашей многолетней страсти к рыбалке и охоте. Ваш богатый жизненный опыт и глубокое понимание природы вызывают искреннее восхищение.

Особенно ценно, что вы из Южно-Сахалинска — региона с уникальными природными богатствами и безграничными возможностями для активного отдыха. Сахалинская земля славится своими рыбными угодьями и охотничьими угодьями, и мы видим в вас настоящего ценителя этих природных сокровищ.

Ваши увлечения говорят о сильном характере, терпении и любви к природе — качествах, которые особенно важны в нашем деле. Мы готовы предложить вам эксклюзивные условия сотрудничества, учитывающие ваш опыт и интересы.

В нашем ассортименте вы найдете специализированное снаряжение для рыбалки и охоты, разработанное с учетом особенностей сахалинского региона. Мы также организуем экспедиции и мероприятия, которые позволят вам полностью погрузиться в мир ваших увлечений.

Не упустите возможность познакомиться с нашими предложениями ближе! Перейдите по ссылке для получения подробной информации: <https://ahotnik.ru>

Мы уверены, что ваши знания и опыт будут ценным вкладом в наше сообщество единомышленников.

С глубоким уважением,
Команда «Охотник»

Рисунок 12 — Пример генерации фишинг письма

На рисунке 13 представлено учебное фишинговое письмо имитирующее уведомление от «управляющей компании» с темой «Внеочередное собрание собственников и ЧП по адресу ул. Комсомольская, 271а», для заместителя генерального директора Глуховой Софьи Павловны в котором фишинговая ссылка была также спрятана через HTML-разметку в гиперссылке в письме.

Софья Павловна, добрый день!

Обращаемся к Вам как к арендатору нежилого помещения по адресу ул. Комсомольская, 271а (ООО «Объединенный расчетный центр»).

Сегодня, в 08:30, в подвальном помещении, смежном с техническим узлом вашего офиса, произошло затопление технической водой с повреждением магистрали. Аварийные службы проводят работы, однако для оценки ущерба и составления акта требуется ваше присутствие или присутствие вашего представителя.

В связи с ЧП, внеплановое собрание для всех арендаторов и собственников здания назначено на сегодня, 09.01.2026, в 14:00 в офисе УК.

Предварительная повестка собрания и схема затопления доступны для ознакомления по [ссылке](#).

Для подтверждения участия и получения пропуска на объект, пожалуйста, заполните краткую [форму](#) в течение часа.

Просим отнестись с максимальной серьезностью. В случае неявки вся ответственность за невозможность оценки ущерба и последующие претензии ляжет на арендатора.

С уважением,
Исполнительный директор УК «Сахалин-Жилком»
А.В. Петров
Конт. тел. диспетчерской: +7 (4242) 84-37-12

Рисунок 13 — Пример учебного фишингового письма для заместителя директора

В случае нажатия на гиперссылку сотрудник попадал на страницу, указывающую переход по фишинговой ссылке, которая представлена на рисунке 14.

Ой-ой! Вы чуть не попали в фишинговую сеть!



Цель этой страницы - показать Вам, как выглядит фишинговая атака, разобрать ключевые признаки подделки и дать четкие инструкции, как действовать в подобных ситуациях.

Что произошло?

Вы кликнули по ссылке, которая имитирует официальный ресурс (банк, соцсеть, сервис электронной почты). В рамках тренингов это учебная ситуация, но в реальной жизни такой переход может привести к:

- утечке логина и паролей;
- краже персональных данных;
- заражению устройства вредоносным ПО;
- потере доступа к аккаунтам.

Как распознать фишинговую ссылку?

1. Подозрительный домен;
2. Отсутствие защищенного соединения;
3. Ошибки в дизайне;
4. Грамматические и стилистические ошибки;
5. Подозрительные формы ввода;
6. Давление и срочность;
7. Отсутствие контактной информации.

Что делать если вы попали на фишинговую страницу?

1. Немедленно закройте вкладку;
2. Не вводите никакие данные;
3. Проверьте устройство на вирусы;
4. Смените пароли;
5. Сообщите о подозрительной ссылке в техническую поддержку.

Помните: лучшая защита от фишинга - это осознанность и пауза перед действием. Если сомневаетесь - не кликайте, а проверьте.

© 2025 Финансовый Тренинг. Все права защищены.

Рисунок 14 — Страница учебной фишинговой ссылки

На данной странице пользователь может увидеть, как в дальнейшем распознавать фишинговую ссылку, а также что необходимо делать если перешел по фишинговой ссылке. При разработке нашей обучающей платформы важно учитывать следующие дидактические принципы [10; 11]:

1. практико-ориентированность — задания должны моделировать реальные рабочие ситуации;
2. постепенное усложнение — сценарии должны адаптироваться к уровню пользователя;
3. регулярность обучения — эпизодические тренинги менее эффективны, чем системная работа;
4. персонализация — учёт должности, уровня цифровых навыков и результатов предыдущих тестов;
5. позитивная мотивация — акцент на обучении, а не на наказании.

Так же применение имитационных атак требует соблюдения этических норм: информирование сотрудников о наличии обучающих кампаний; запрет на публичное раскрытие индивидуальных ошибок; использование результатов исключительно в образовательных целях; защита персональных данных. Педагогическая цель обучения, заключается в формировании компетенций, а не в выявлении «слабых звеньев» [12; 13].

Использование тренировочных фишинговых ссылок представляет собой метод ситуационного обучения. Его педагогическая ценность заключается в следующем [14; 15]:

1. Формирование навыка через действие. Сотрудник не просто слушает теорию, а принимает решение в условиях, приближённых к реальности.
2. Мгновенная обратная связь. При переходе по тренировочной ссылке пользователь перенаправляется на обучающую страницу с разбором признаков фишинга.
3. Эмоциональное вовлечение. Осознание собственной ошибки усиливает запоминание и способствует формированию устойчивого поведения.
4. Развитие критического мышления. Анализ письма и выявление подозрительных признаков формируют аналитические навыки.

Таким образом, фишинговая симуляция становится не инструментом контроля, а средством формирования цифровой культуры.

Заключение.

Создание платформы для обучения сотрудников защите от фишинга с использованием имитационных фишинговых ссылок представляет собой современный образовательный инструмент, основанный на принципах практико-ориентированного и адаптивного обучения.

Переход от формального информирования к моделированию реальных ситуаций позволяет сформировать устойчивые навыки безопасного поведения в цифровой среде.

Таким образом, эффективная защита организации от фишинговых атак начинается не только с технологий, но прежде всего с педагогически выстроенного процесса формирования цифровой культуры сотрудников.

«PhishingTrainer» — это не просто инструмент обучения, а система формирования культуры информационной безопасности в организации. Внедрение такой платформы позволяет:

1. минимизировать риски, связанные с человеческим фактором;
2. повысить устойчивость бизнеса к кибератакам;
3. создать проактивную защиту на основе постоянного развития компетенций персонала.

Внедрение платформы является важным шагом для любой организации, стремящейся к улучшению своей безопасности. Это дает возможность не только обучать сотрудников, но и создать культуру осведомленности о киберугрозах. Отсутствие знаний о фишинге может

привести не только к возможным утечкам данных, но и к серьезным финансовым потерям для компании. Использование фишинговых симуляций как метода обучения предоставляет сотрудникам необходимые навыки для распознавания и предотвращения потенциальных угроз, что незаменимо в современных условиях.

Плюсы такого обучения: персонализация обучения, максимальная эффективность, адаптивность и аналитика результатов.

Рассмотрим ключевые итоги нашего исследования. Так как актуальность проблемы фишинга не снижается и по сей день. Человеческий фактор остаётся главным уязвимым звеном в системе киберзащиты, а традиционные методы обучения демонстрируют недостаточную эффективность.

Инновационность нашего подхода заключается в применении машинного обучения для автоматической генерации реалистичных фишинговых сценариев, персонализации учебных материалов под конкретного сотрудника и динамической адаптации сложности заданий.

Комплексная архитектура платформы «PhishingTrainer» обеспечивает замкнутый цикл обучения от симуляции атаки до анализа результатов и выдачи персональных рекомендаций.

Практическая эффективность решения подтверждается возможностью снизить количество успешных фишинговых атак на 60–80 %. Также сформировать устойчивые навыки распознавания угроз и получить объективную оценку уровня киберграмотности персонала.

Стратегическая значимость обучающей платформы «PhishingTrainer» состоит в том, что переводит обучение из формата разовых мероприятий в постоянный процесс и выводит на системность обучения. Создаёт «человеческий файрвол» — команду сотрудников, способных оперативно реагировать на киберугрозы. Обеспечивает измеримый результат через детальную аналитику и отчётность.

Перспективы развития платформы «PhishingTrainer» связаны с интеграцией передовых генеративных моделей ИИ для создания ещё более изощрённых сценариев социальной инженерии.

Планируем добавить механизмов геймификации для повышения вовлечённости. Например, публикация визуализация учебного процесса, таблиц лидеров, награды за прохождения сложных сценариев, квесты, миссии, соревнование и другое.

Разработка мобильных решений для обучения вне рабочего места, что обеспечит доступность обучения в любое месте и в любое время. Добавиться интеграция с корпоративными мессенджерами, AR-элемент (сканирование QR кода).

Список источников:

1. Другач Ю.С. Контролируемый взлом. Библия социальной инженерии. - 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2024. - 208 с.
2. Шубина Э. Е., Никитина Е.Ю. Исследование обучения персонала защите от фишинга и оценка их уязвимости // Актуальные проблемы информационной безопасности: Сборник статей. – Пермь: Пермский государственный национальный исследовательский университет, 2025. – С. 140-146. URL: <https://www.elibrary.ru/sryvum>
3. Ефимов С.А., Пронькин Н.Н. Роль сотрудников в обеспечении информационной безопасности: подходы к повышению осведомлённости // International Journal of Professional Science. 2024. № 6-2. С. 40-47. URL: <https://www.elibrary.ru/evqrijk>
4. Прохоров А.И., Маркин Е.А., Никеева У.Г. Фишинг – атаки: основные виды и способы защиты от них // Информационные системы, экономика и управление. Ученые записки. Ростов-на-Дону, 2023. С. 84-90. URL: <https://www.elibrary.ru/mzgipec>

5. Бачиева А.В., Бозиев Т.О. Фишинг как один из способов мошенничества в сфере компьютерной информации // В сборнике: Актуальные проблемы юридической науки и практики. – Гатчина: Государственный институт экономики, финансов, права и технологий. - С. 232-235. URL: <https://www.elibrary.ru/zhtgzh>
6. Захарова А.А. Методы обучения персонала в организации // Аллея науки. 2022. Т. 1, № 3 (66). С. 114-120. URL: <https://www.elibrary.ru/acjlnb>
7. Ан Д. С., Зуфарова А.С. Симуляция фишинговых атак как метод повышения киберграмотности и подготовки к реагированию на угрозы // Управление образованием: теория и практика. 2025. № 6-1. С. 127-139. URL: <https://www.elibrary.ru/zbcsvm>
8. Зуфарова А.С. Интеграция искусственного интеллекта в современное образование: преимущества и вызовы // ЦИТИСЭ. 2025. № 1. С. 652-659. URL: <https://www.elibrary.ru/vmftaa>
9. Жданова Д.Е. Технология реверсивного обучения: сочетание мобильного обучения и активных методов обучения // Наукосфера. 2021. № 7-1. С. 55-58. URL: <https://www.elibrary.ru/siqyud>
10. Нечипуровский Д.И. Как построить многоуровневую защиту для борьбы с продвинутыми угрозами фишинга // Научный аспект. 2024. Т. 41, № 4. С. 5337-5342. URL: <https://www.elibrary.ru/jdtfvy>
11. Яковлева М.А. Лидерство в системе наставничества как эффективный инструмент адаптации персонала // Human Progress. 2021. Т. 7, № 1. URL: <https://www.elibrary.ru/mfmyr>
12. Сливинский Д.В., Шишияну К.С. Обучение персонала как технология управления человеческими ресурсами предприятия: основные формы, методы и критические оценки // Инновации и инвестиции. 2023. № 11. С. 78-80. URL: <https://www.elibrary.ru/bwijwi>
13. Байкулова Ф.Р. Разработка методики выявления фишинговых атак // Студенческий вестник. 2024. № 23-6(309). С. 57-59. URL: <https://www.elibrary.ru/egoqxc>
14. Ченушкина С.В. Шмакова Л.Е. Роль визуализации в формировании компетентности в области кибербезопасности // Мир науки, культуры, образования. 2023. № 6(103). С. 229-233. URL: <https://www.elibrary.ru/wshgmi>
15. Лебедева Д. А., Виткова Л.А. Анализ эффективности методов защиты от фишинга // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2025. № 2. С. 100-104. URL: <https://www.elibrary.ru/gmsped>

References:

1. Drugach, Yu. S. (2024). *Controlled hacking. The Bible of social engineering (2nd ed., revised and enlarged)*. BHV-Petersburg. (In Russian).
2. Shubina, E. E., & Nikitina, E. Yu. (2025). Study of personnel training in protection against phishing and assessment of their vulnerabilities. In *Actual problems of information security: Collection of articles* (pp. 140–146). Perm State National Research University. (In Russian). <https://www.elibrary.ru/sryvum>
3. Efimov, S. A., & Pronkin, N. N. (2024). The role of employees in ensuring information security: Approaches to raising awareness. *International Journal of Professional Science*, 6–2, 40–47. (In Russian). <https://www.elibrary.ru/evqrjk>
4. Prokhorov, A. I., Markin, E. A., & Nikeeva, W. G. (2023). Phishing attacks: Main types and methods of protection against them. In *Information systems, economics and management: Scientific notes* (pp. 84–90). Rostov-on-Don. (In Russian). <https://www.elibrary.ru/mzgiqc>
5. Bacheva, A. V., & Boziev, T. O. (2023). Phishing as one of the methods of fraud in the field of computer information. In *Actual problems of legal science and practice* (pp. 232–235).

State Institute of Economics, Finance, Law and Technology. (In Russian).
<https://www.elibrary.ru/zhtgzh>

6. Zakharova, A. A. (2022). Personnel training methods in an organization. *Alley of Science, 1*(3), 114–120. (In Russian). <https://www.elibrary.ru/acjlnb>

7. An, D. S., & Zufarova, A. S. (2025). Simulation of phishing attacks as a method of improving cyberliteracy and preparing for response to threats. *Education Management: Theory and Practice, 6–1*, 127–139. (In Russian). <https://www.elibrary.ru/zbcsvm>

8. Zufarova, A. S. (2025). Integration of artificial intelligence in modern education: Advantages and challenges. *CITISE, 1*, 652–659. (In Russian). <https://www.elibrary.ru/vmftaa>

9. Zhdanova, D. E. (2021). Reverse learning technology: A combination of mobile learning and active learning methods. *Naukosphere, 7–1*, 55–58. (In Russian). <https://www.elibrary.ru/siqyud>

10. Nechipurovsky, D. I. (2024). How to build a multi-layered defense to combat advanced phishing threats. *Scientific Aspect, 41*(4), 5337–5342. (In Russian). <https://www.elibrary.ru/jdtfvy>

11. Yakovleva, M. A. (2021). Leadership in the mentoring system as an effective tool for personnel adaptation. *Human Progress, 7*(1). (In Russian). <https://www.elibrary.ru/mfmyrr>

12. Slivinsky, D. V., & Shishyanu, K. S. (2023). Personnel training as a technology for managing the human resources of an enterprise: Basic forms, methods, and critical assessments. *Innovations and Investments, 11*, 78–80. (In Russian). <https://www.elibrary.ru/bwijwi>

13. Baykulova, F. R. (2024). Development of a methodology for detecting phishing attacks. *Student Bulletin, 23–6*(309), 57–59. (In Russian). <https://www.elibrary.ru/egoqxc>

14. Chenushkina, S. V., & Shmakova, L. E. (2023). The role of visualization in forming competence in cybersecurity. *The World of Science, Culture, Education, 6*(103), 229–233. (In Russian). <https://www.elibrary.ru/wshgmi>

15. Lebedeva, D. A., & Vitkova, L. A. (2025). Analysis of the efficiency of anti-phishing protection methods. *Bulletin of the St. Petersburg State University of Technology and Design. Series I: Natural and Technical Sciences, 2*, 100–104. (In Russian). <https://www.elibrary.ru/gmsped>

Submitted: 16 February 2026

Accepted: 16 March 2026

Published: 17 March 2026

